УДК 343.98

НЕКОТОРЫЕ ОСОБЕННОСТИ РАБОТЫ С ЭЛЕКТРОННО-ЦИФРОВЫМИ СЛЕДАМИ ПРИ РАССЛЕДОВАНИИ СКЛОНЕНИЯ НЕСОВЕРШЕННОЛЕТНЕГО К САМОУБИЙСТВУ, СОВЕРШЕННОГО В СЕТИ ИНТЕРНЕТ

С. В. Мосина
кандидат юридических наук,
начальник кафедры криминалистики
Уральского юридического института МВД России (г. Екатеринбург)
В. Ю. Иванов
адъюнкт адъюнктуры
Уральского юридического института МВД России (г. Екатеринбург)

Авторы анализируют особенности производства следственных действий по изъятию и осмотру электронно-цифровых следов при расследовании преступлений, связанных со склонением несовершеннолетних лиц к самоубийству, совершаемых посредством информационно-телекоммуникационных технологий. В статье приведены рекомендации по изъятию технических устройств и копированию криминалистически значимой информации с них в условиях противодействия со стороны жертвы преступного посягательства. Обосновывается важность выстраивания психологического контакта с потерпевшим от преступления, и аргументируется целесообразность добровольного изъятия электронно-цифровой информации с мобильных телефонов и компьютерных устройств несовершеннолетнего. Предлагается тактический прием, позволяющий произвести копирование компьютерной информации в условиях неосведомленности владельца технического устройства посредством аппаратно-программных комплексов.

Ключевые слова: *самоубийство, склонение, электронно-цифровые следы, компьютерная информация, техническое устройство, изъятие, сеть Интернет, социальные сети, «группы смерти».*

Относительно недавно в законодательство Российской Федерации была введена норма, устанавливающая уголовную ответственность за действия, направленные на склонение несовершеннолетнего к самоубийству или содействие в совершении самоубийства с использованием сети Интернет. Предпосылкой этому послужило появление и интенсивное развитие так называемых групп смерти, осуществляющих свою незаконную деятельность, как правило, в социальной сети «ВКонтакте». Среди наиболее популярных по количеству участников выделяют такие группы, как: «Тихий дом», «Разбуди меня в 4:20», «Синий кит». Существуют и менее популярные общественные объединения в социальных сетях, преследующие аналогичные мотивы.

Основной целью данных групп является склонение к совершению самоубийства ребенка посредством выполнения им различных заданий, передаваемых «куратором» группы. Как правило, задания строятся по принципу от условно простых (например, залезть на крышу здания и встать на карниз) к более сложным (например, перебежать дорогу перед двигающимся с большой скоростью автомобилем). В начале «игры» общение с ребенком строится с налаживания психологического контакта. Весь период «игры» длится от нескольких дней до 1–2 месяцев, в зависимости от психологической устойчивости ребенка. В конце «игры», когда «куратор» приходит к выводу, что ребенок психологически готов добровольно уйти из жизни, ему высылается последнее задание, связанное с совершением самоубийства.

Если поставленная задача не была выполнена, то в адрес несовершеннолетнего могут поступать сообщения, содержащие угрозы физической расправы над ним и его семьей, в целях запугивания жертвы и подталкивания к совершению суицида. Указан-

ные обстоятельства свидетельствуют о том, что именно на данной стадии необходимо выявить преступление, чтобы предупредить возможные негативные последствия.

Актуальность проблемы также подтверждается статистическими данными, указывающими на увеличение количества детских самоубийств. Так, за последние два года общий прирост составил почти 14 % [1].

Так, Рина Паленкова 17 лет из Уссурийска покончила жизнь самоубийством, добровольно положив свою голову на железнодорожные рельсы перед приближающимся с большой скоростью грузовым поездом. Машинист заметил девушку в самый последний момент, вследствие чего экстренное торможение не позволило избежать трагедии. Перед смертью несовершеннолетняя девушка сделала последнее в своей жизни «селфи» на фоне железной дороги [2].

Данный пример позволяет сделать вывод о том, что основную криминалистически значимую информацию содержат электронно-цифровые следы, содержащиеся в компьютерной технике и мобильных устройствах жертв.

Данный тезис также обусловлен тем, что преступники в подавляющем большинстве случаев не вступают в прямую коммуникацию с жертвой, а осуществляют воздействие на нее при помощи текстовых сообщений и отправки различных медиафайлов [3, с. 45].

Учитывая то, что подростки, которые становятся жертвами рассматриваемых преступлений, блокируют доступ к информации, содержащейся на личных страницах в социальных сетях, при расследовании особое внимание следует уделять налаживанию психологического контакта с несовершеннолетним потерпевшим. Важно понимать, что на протяжении длительного времени с ним работали «кураторы», выстраивающие общение по определенной методике, которые успели войти в доверие к ребенку и внушить необходимость сохранения тайны переписки. Как правило, такие дети отличаются повышенной раздражимостью, замкнутостью, наличием странностей в поведении и т. д.

В частности, на первоначальном этапе расследования необходимо получить доступ к возможной переписке и переговорам подростка с посторонними лицами, в том числе к данным, хранящимся в социальных сетях [4, с. 52]. При этом следует находить грань между способами получения криминалистически значимой информации, способствующей эффективному раскрытию и расследованию преступления, и психофизиологическими особенностями подросткового возраста, обусловленными «подростковыми комплексами», связанными с повышенной чувствительностью к оценке окружающих, частой сменой настроения, отсутствием собственного устоявшегося мнения и т. д.

Исходя из указанного, следует учитывать, что в случае отказа ребенка предоставить правоохранительным органам или родителям личную переписку с «куратором», необходимо оградить его от дальнейшего пользования социальными сетями во избежание повторного контакта с участниками «групп смерти». Следует продолжить налаживание психологического контакта, постепенно входя в доверие к подростку. Для общения необходимо привлекать детского психолога, который сможет выстроить правильный подход к ребенку. Это позволит без принуждения получить доступ к техническому устройству, через которое происходило общение с «куратором».

Следующей актуальной проблемой, возникающей при расследовании преступлений, связанных со склонением несовершеннолетнего к самоубийству с использованием сети Интернет, является отсутствие качественной работы со стороны правоприменителя с электронно-цифровыми следами преступления. Как указывалось ранее, именно они являются основным источником криминалистически значимой информации. И если ранее изучение содержимого внутренней памяти мобильного телефона могло быть произведено без использования каких-либо технических средств, то в настоящее время без специального оборудования крайне сложно решить данную задачу. Помимо этого, ранее удаленную информацию невозможно извлечь из памяти устройства без специальных аппаратных и программных средств [5, с. 110].

Несмотря на то, что современные достижения в области получения информации, например аппаратно-программные комплексы «Мобильный криминалист», «UFED», «Secure View 3», «MOBILedit!», «MicroSystemation», «XRY» и другие, позволяют оперативно получить необходимую информацию, при расследовании рассматриваемых преступлений не рекомендуется производить принудительное изъятие содержимого переписок и иной информации, хранящейся в телефоне или компьютерном устройстве.

Недобровольное изъятие криминалистически значимой информации может привести к куда более нежелательным последствиям [6, с. 68]. Стоит учитывать, что подросток определенное время был подвержен негативному психологическому воздействию «куратора», направленному на совершение самоубийства. Принудительное изъятие информации, находящейся в личных переписках, может непредсказуемым образом повлиять на психологическое или даже на психическое состояние ребенка и его дальнейшие действия.

В то же время ввиду портативности данных аппаратно-программных комплексов возможно применение тактического приема по копированию содержимого мобильного устройства без непосредственного согласия собственника. Для этого достаточно подключить интересующее техническое устройство к ноутбуку с заранее предустановленным программным обеспечением «Мобильный криминалист» или «UFED». Сложность может возникнуть, если устройство имеет пароль, а также обладает большим объемом заполненной памяти. Все это значительно увеличивает время, требуемое для декодирования устройства и копирования файлов. По этой причине данный тактический прием применим лишь в условиях, когда внутренняя память телефона занимает небольшой объем, а техническое устройство не обладает паролем для доступа к внутреннему содержимому.

Электронно-цифровые следы преступления, как правило, содержатся в перепи-сках несовершеннолетнего с «куратором». Все общение происходит посредством мессенджеров (например, WhatsApp, Viber, Telegram) и социальных сетей («ВКонтакте», Instagram, TikTok и др.). Стоит принимать во внимание, что современные дети все чаще для общения предпочитают использовать мобильные устройства, пренебрегая персональным компьютером или ноутбуком. Поэтому нельзя ограничиваться исследованием лишь данных технических устройств.

В настоящее время модельный ряд компьютерной техники достаточно разнообразен и продолжает расширяться. Каждая новая модель совершенствуется, операционная система становится менее уязвимой, вследствие чего не с любой моделью представляется возможным работать с помощью аппаратно-программного комплекса. Однако разработчики постоянно совершенствуют данные комплексы, что позволяет получать больше криминалистически значимой информации.

Опираясь на практический опыт, можно выделить основополагающие принципы работы с техническими устройствами, содержащими электронно-цифровые следы:

– следует обеспечить качественную сохранность следов (исключить доступ к информации посторонних лиц, осуществлять контроль за бесперебойностью работы компьютерного оборудования);

– не допускается поиск файлов и работа с ними на включенном устройстве без участия соответствующего специалиста;

– в случае необходимости изъятия компьютерного оборудования осуществляется правильное завершение работы, отключается роутер или модем;

– если есть угроза несанкционированного уничтожения электронно-цифровых следов преступления вредоносным программным обеспечением, принимаются меры к экстренному отключению компьютера от сети электропитания;

– в случае осуществления осмотра устройства, работающего от аккумуляторной батареи, например ноутбука, следует принять меры по ее отсоединению, при этом стоит учитывать, что существуют устройства с цельным корпусом, где без специальных инструментов достать аккумуляторную батарею не представляется возможным;

– осуществляется тщательный контроль за упаковкой и транспортировкой изъятого оборудования;

– производство осмотра компьютера сопровождается фотофиксацией его внешнего вида, отображения экрана монитора и подключенных к нему устройств;

– производится фотофиксация и подробное описание обстановки возле технического устройства;

– запрещается приводить в рабочее состояние выключенное устройство без участия соответствующего специалиста;

– каждый изымаемый объект подлежит индивидуальной маркировке;

– упаковка должна исключать возможность повреждения изъятых предметов;

– обеспечивается транспортировка и дальнейшее хранение в условиях, исключающих контакт с магнитами и другими потенциально опасными устройствами;

– любая документация, связанная с исследуемым оборудованием (записи, содержащие логины, пароли и т. п.), подлежит обязательному изъятию;

– при работе с включенным мобильным телефоном или планшетом недопустимо выключать или блокировать экран; повторное включение может привести к запросу пароля, что осложнит работу с данными; при этом необходимо обеспечивать заряд аккумуляторной батареи в оптимальном состоянии;

– если по каким-либо причинам устройство не может длительное время поддерживать автономную работу без дополнительного заряда батареи, а зарядное устройство отсутствует, то необходимо незамедлительно организовать работу с данным устройством с участием специалиста до того, как оно разрядится;

– необходимо своевременно осуществлять детальное документирование всех произведенных действий в соответствующем протоколе осмотра места происшествия.

Подводя итог, можно заключить, что поиск способа изъятия электронно-цифровых следов при производстве следственных действий с участием несовершеннолетних при расследовании преступлений, связанных с их склонением к самоубийству или содействием в совершении самоубийства, совершенных в сети Интернет, имеет важную роль. Работа с несовершеннолетним потерпевшим требует от правоприменителя знания не только процессуальных норм, но и тактических приемов, а также психологических особенностей поведения подростков. Поспешные решения могут стать причиной нежелательных последствий как для процесса расследования уголовного дела, так и для потерпевшей стороны. Грамотно выстроенные действия в процессе расследования уголовного дела могут способствовать эффективному раскрытию и расследованию преступления. Существенную роль в осмотре и изъятии криминалистически значимой информации с технических устройств играют аппаратно-программные комплексы, о чем свидетельствует их востребованность при расследовании преступлений, совершенных с помощью IT-технологий.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Официальный сайт Следственного комитета РФ [Электронный ресурс]. — Режим доступа: https://sledcom.ru/press/interview/item/1276735/?pdf=1. — Дата доступа: 19.11.2020.

2. Девушка из Уссурийска покончила жизнь самоубийством бросившись под поезд [Электронный ресурс]. — Режим доступа: https://nalchik.bezformata.com/listnews/rina-palenkova-pitalas-vizhit/40820471/. — Дата доступа: 23.11.2020.

3. Ганишев, П. А. Виктимологические особенности личности потерпевшего от преступления предусмотренного п. «д» ч. 3 ст. 110.1 УК РФ / П. А. Ганишев // Вестн. Всерос. ин-та повышения квалификации сотрудников М-ва внутр. дел Рос. Федер. — 2020. — № 1 (53). — С. 43–46.

4. Хлобыстова, П. Ю. О разработке методики расследования склонения к совершению самоубийства или содействия совершению самоубийства / П. Ю. Хлобыстова, И. Н. Колчина // Фундаментальные и прикладные научные исследования: актуальные вопросы, достижения и инновации : VIII Междунар. науч.-практ. конф. — Пенза, 2017. — С. 50–52.

5. Кормильцин, С. Г. Об использовании аппаратно-программного комплекса UFED Touch при осмотре мобильных устройств связи / С. Г. Кормильцин // Расследование преступлений: проблемы и пути их решения. — 2019. — № 1 (23). — С. 109–112.

6. Файрушина, Р. Д. Особенности производства следственных действий по изъятию и осмотру компьютерной информации / Р. Д. Файрушина // Вестн. Уфим. юрид. ин-та МВД России. — 2017. — № 3. — С. 67–70.

Поступила в редакцию 16.11.2020 г.
Контакты: svetlana-p-v@mail.ru (Мосина Светлана Вячеславовна),
blad02051995@mail.ru (Иванов Владислав Юрьевич)

Mosina S. V., Ivanov V. Yu.

SOME FEATURES OF WORKING WITH ELECTRONIC-DIGITAL TRACKS IN INVESTIGATING THE DECLINATION OF A MINOR TO SUICIDE, COMMITTED ON THE INTERNET

The authors analyze the peculiarities of the production of investigative actions for the seizure and inspection of electronic digital traces in the investigation of crimes related to persuading minors to commit suicide by means of information and telecommunication technologies. The article provides recommendations for the removal of technical devices and copying of forensically significant information from them. The importance of building psychological contact with the «victim» of the crime is substantiated and the expediency of voluntary withdrawal of electronic digital information from mobile phones and computer devices of the victim is argued.

Keywords: *suicide, declination, digital traces, computer information, technical device, seizure, the Internet, social networks, death groups.*